HYTRUST | intel

White Paper

Banking on **Cybersecurity**

Best practices to strengthen data security and regulatory compliance in financial services

The financial services industry was hit by its most significant cyber attack to-date in 2014 at a top five global bank. Hackers stole the highest level of administrator privileges for over 80 servers, gaining unlimited access to 83 million personal and business records. However, this massive cyber breach could have been stopped in its tracks if the banking giant had implemented one simple, but powerful, cybersecurity best practice. Even though the bank had spent $250 million to fortify its cyber defense, it had failed to add two-factor authentication, which requires two forms of identification for system access.

This opportunistic cyber breach of a financial services organization is not an anomaly. Cyber attacks are becoming more frequent, more powerful, and more clever every year. In 2016, the financial sector was attacked more than any other industry, according to the 2017 IBM X-Force Threat Intelligence Index, with the average financial services firm experiencing 65 percent more attacks than the average non-financial organization. Despite spending millions of dollars on defense, most financial organizations remain at risk of external and internal data breaches, attacks, and mistakes.

Financial services firms' data is appealing to cyber criminals because it can be quickly monetized in underground marketplaces, including selling consumers' Personal Identifiable Information (PII). Along with malicious breaches, data is also at risk for system administrator mistakes. The potential damage and disruption from successful data breaches or accidents can be catastrophic—including loss of revenue, erosion of consumer confidence, regulatory penalties, and business closures. Moreover, these incidents can also threaten the stability of the global financial system, according to the Office of Financial Research.

For these reasons, cybersecurity is one of the top priorities for regulatory agencies. In today's high-risk environment, they're setting strict security rules, standards, guidelines, and frameworks to strengthen cybersecurity policies and prevent attacks. Penalties for non-compliance can be high. Yet, many financial services organizations lack robust continuous compliance programs.

While financial services firms are spending millions on cybersecurity systems, too often they still overlook critical best practices tailored to defend against the five most common security challenges. In particular, they fail to realize that in an increasingly virtualized world, traditional security measures and technologies are no longer adequate. Traditional cybersecurity practices must be reinforced with tools and technologies that are born in the cloud. By adopting cloud-based security best practices that mitigate the risks of malicious attacks and accidents, financial services organizations can achieve three critical cyber defense goals—mitigate cybersecurity risks, improve regulatory compliance, and secure all data wherever it resides.

General

Cybercrime has jumped to the second-most reported economic crime and financial organizations are prime targets – *PWC's Global Economic Crime Survey*

Financial services encounter security incidents 300% more frequently than other industries – *Websense's 2015 Industry Drill-Down Report: Financial Services*

66.2% of financial organizations faced at least one cybersecurity attack in 2016 – *MetricStream Research's The State of Cybersecurity in the Financial Services Industry*

Cyber attacks against the financial services industry are increasingly sophisticated and frequent. With 45% of financial services firms experiencing between one and five breaches in 2016 – *High Performance Security Report*

86% of financial services firms plan to spend more time and resources on cybersecurity in 2017 versus just 60% in 2016 – *Duff & Phelps Global Enforcement Review 2017*

72% of respondents in the banking and financial services industry cited cyber threats as a top risk, far ahead of other industry averages at 54% – *2016 Travelers Risk Index*

50% of respondents in financial services expressed concern about the potential for theft or loss of control of the company's customer or client records – *Duff & Phelps Global Enforcement Review 2017*

The U.S. bank with the weakest security posture is one of the top 10 largest financial service organizations in the U.S (by revenue) – *2016 Financial Industry Cybersecurity Report*

Recent cyber attacks have highlighted concerns about the potential of an even more destructive incident that could significantly disrupt the financial system – *U.S. Financial Stability Oversight Council*

Major Cyber Attacks in Financial Services

Cyber criminals go where the money is. That's why some of the biggest breaches have occurred in the financial services industry. On top of daily phishing, malware, and ransomware attacks, in 2016, financial services organizations faced 85 serious attempts to breach their cyber-defenses. Over 36 percent of the attacks succeeded in stealing data, according to the Accenture High-Performance Security Report 2016.

Here are just of few of the most devastating financial services cyber attacks in the past several years. While they represent just the tip of the financial industry's cyber breach iceberg, together they illustrate the very real vulnerabilities financial services organizations experience on a daily basis.

Organization	Attack Date	Cyber Attack Method	Damages
Society for Worldwide Interbank Financial Telecommunication (SWIFT)	2016	Obtained valid bank employee credentials, which they used to conduct money transfers and initiate money transactions from multiple banks	See Bank of Bangladesh breach below
Bank of Bangladesh	2016	Used SWIFT credentials to transfers funds to bank accounts in Asia	$81M (attempted $1B)
Scottrade	2012-2015	Accessed Scottrade (along with online stock brokerages in Nebraska, New York, and North Carolina) by accessing several vulnerable attack points	Accessed 4.6M customers' records
Charles Schwab	2016	Breached by an unauthorized person who obtained a client's username and password, then logged into user accounts, exposing names, account numbers, stock positions, and transaction history	Potentially all customers
UniCredit (Italy)	2016-2017	Gained unauthorized access to customer biographical and loan data through an outside company employed by the bank	400K clients
Heartland Payment Systems	2015 (second breach)	Stole password protected computers, and accessed unencrypted data	$140M in fines and other penalties
Global Payments	2011	Took advantage of weak server configurations to inject malicious code into the database behind the public-facing Web server; they uploaded software and siphoned data	Potentially 7M Visa and MasterCard accounts, and $100M
'Top 5 Global Bank'	2011	Used vulnerabilities in customer-facing website as a gateway to bypass traditional safeguards and impersonate actual credit card holders' accounts	360,000 credit card holders' data, and $19.4M
Heartland Payment Systems	2006-2008 (first breach)	Infiltrated computer networks; credit and debit cards stolen, then sold and used to make unauthorized purchases and bank withdrawals	134M credit cards stolen

Data Security Risks and Breaches

Financial services is one of the top 3 industries experiencing cyber attacks – *Verizon Breach Report 2016*

Over 66% of financial services firms experienced breaches in 2016 – *MetricStream*

In 33% of data breach attempts against financial services firms, the attackers succeeded – *Accenture*

The finance industry ranked #1 for security incidents with confirmed data loss – *2016 Verizon Data Breach Report*

83% of financial services firms cite defending against cyber threats and protecting personal data as one of their biggest challenges in building or maintaining their reputation – *2015 Makovsky Wall Street Reputation Study*

95% of the top 20 U.S. commercial banks were graded "C" or worse for network security – *SecurityScorecard's 2016 Financial Industry Cybersecurity Report*

The cost of a single cyber security incident in the U.S. can be as much as $1,165,000 – *Kaspersky Lab's Financial Institutions Security Risks Survey*

The average dollar cost of a breach is reported to be $4 million – *Ponemon Institute's "Cost of Data Breach Study 2017"*

Financial firms take an average 98 days to detect breach, leaving attackers unimpeded inside the network able to inflict significant damage — *Ponemon Institute's "Advanced Threats in Financial Services and Retail" study*

Key Security Challenges in Financial Services

While working to deliver local, national, or global financial services, organizations face a myriad of security challenges—including data security breaches, both malicious and accidental insider threats, multi-cloud deployments, emerging technology vulnerabilities, and consistent regulatory compliance and audit risk.

1. Multi-Cloud Deployment Management. Like companies in other industries, financial services organizations are racing to take advantage of cloud computing opportunities. Cloud adoption business drivers include: scalability (51%), business agility (46%), and cost (43%), according to North Bridge's Future of Cloud Computing Survey. Despite the substantial benefits, many financial services organizations are wary of moving into multi-cloud environments. The fear of data breaches in third-party environments remains the number one barrier to cloud service adoption—because while organizations can outsource functionality, they cannot outsource their data security responsibility.

2. Data Security Breach Risks. Cyber attacks against the financial services industry are increasingly sophisticated and frequent. In the face of ever-present risks, organizations must protect their customers' PII, as well as confidential business information and intellectual property. Any data loss results in a cascade of problems—from regulatory scrutiny to class action lawsuits. But there is a flip side to cyber defense. Organizations that have not experienced data breaches may have created excessively restrictive policies, particularly around cloud adoption. This restrictive posture can unnecessarily restrict business development.

3. Insider Threats. Malicious and Accidental. While most cybersecurity systems are designed to keep criminals out, many organizations have not planned for insider threats. Whether malicious or accidental, insiders can cause severe damages, including devastating data leaks, payment transfers, illegal trades, and security code exploitation. In fact, attacks from within often cause the most damage, according to SANS Institute. Insider threats are made worse when organizations have not properly configured system and network access levels to align with employees' levels of authority and job responsibilities. In fact, privileged users typically have access to all resources and systems in the cloud, unless otherwise restricted by security controls. These human points of interaction have the potential to undermine even the most comprehensively designed cybersecurity systems with a single malicious or accidental act.

4. Emerging Technologies Compound Security Challenges. As financial institutions shift to digital channels like online banking, mobile transactions, and the Internet of Things (IoT), their digital footprints expand and their cyber attack surface widens. The more virtual channels organizations provide to customers, the more potential routes cyber criminals have with which to breach their security defenses. Willis Group Holdings, a leading global risk advisor, noted: "Given the interconnectivity of the internet, today's rapid digital advances, and social media platforms, a cyber crisis at one or more banks can result in financial catastrophe, not only to customers and banks, but also to the country's financial system as a whole."

5. Financial Institutions Face Multiple Compliance Regulations. Among the many negative consequences of Heartland Payment Systems' data breach was being deemed non-compliant with the Payment Card Industry Data Security Standard (PCI DSS). The firm's penalties included being banned from processing payments of major credit card providers for several months and paying an estimated $145 million in compensation for fraudulent payments. Similarly, in September 2015, the SEC reached a settlement with a St. Louis-based investment adviser on charges that it failed to establish required cybersecurity policies and

Insider Threats – Malicious and Accidental

Over 48% of financial services organizations reported that employees are the primary conduits through which cyber attacks are launched – *MetricStream's The State of Cybersecurity in the Financial Services Industry*

19% believe the potential loss from an insider threat is more than $5 million, and another 15% valued the loss at $1 to $5 million – *SANS Institute*

One-third of enterprises have suffered from an insider-caused breach, with possible losses from each incident amounting to more than $5 million – *SANS Institute*

Only 17% of security professionals were aware of insider threats on their network, even though enough anomalous activity suggested that insider threats occurred in 85% of organizations – *Institute for Critical Infrastructure Technology*

The FBI and Department of Homeland Security agree that insider threats have increased and that such threats pose a serious risk

In 2016, most attacks against financial services firms were unknowingly facilitated by "inadvertent actors" – *IBM*

procedures before a breach affected the PII of 100,000 clients stored on a third party-hosted web server. R.T. Jones agreed to cease and desist, be censured, and pay a $75,000 penalty. These are just two examples of the penalties financial services organizations incur when they fall out of compliance with one or more of the industry's leading compliance regulations. In addition to being in the crosshairs of cyber attacks, financial services organizations face a growing number of stringent industry and government regulations. Some of the regulations carry potentially firm-destroying consequences, such as the European General Data Protection Regulation (GDPR) in which firms may be penalized up to four percent of their global annual revenue for non-compliance. (See addendum for list of financial services compliance agencies.)

Best Practices for Security and Compliance in Financial Services

To mitigate the risks associated with the aforementioned security challenges, including meeting compliance regulations, financial services organizations must implement specific cybersecurity best practices. The following eight best practices are designed to strengthen cybersecurity through strong data encryption and key management, ironclad access controls, and continuous data visibility and monitoring. They'll also help meet today's wide range of state, federal, and international data privacy compliance regulations.

Best Practice 1: Strong Encryption

Encryption is a mechanism used to protect and obfuscate data by transforming it into an unreadable format so it remains private from anyone or anything not explicitly approved to read it through decryption. An individual or application that needs access to encrypted information must possess the correct secret code—called a "key"—to convert the data back to its original readable format. In this way, encryption provides a fail-safe mechanism whereby, if all other security measures fail and data is in fact stolen, the information is still protected, as it is unreadable and thus useless. The Cloud Security Alliance reported that data encryption is playing an expanding role in the financial services industry, both for securing in-house computing and for migration to the cloud. It expects to see deployment numbers rise.

Best Practice 2: Strong Key Management

Even the best encryption practices are only as good as an organization's ability to protect its decryption keys. In encrypted environments, decryption keys effectively act as proxies for the data they protect. If the keys are compromised, so is the data. Simply stated, keys are equivalent to the series of numbers that open locked bank safes. If a thief knows a safe's combination, even the strongest safe in the world provides no real security. Organizations must efficiently manage their decryption keys throughout the key lifecycle, including generating, distributing, storing, rotating, and revoking keys.

Best Practice 3: Role-Based Access Control (RBAC)

Too often, organizations give unlimited yet unnecessary access of systems and data to privileged admins, especially in the cloud. As a result, in a few mistaken mouse clicks an admin can suspend, copy, or delete virtual workloads, alter network configurations, or bring hypervisors out of compliance. RBAC can reign in this risk by restricting admins to only performing certain operations or only operating on certain workloads that pertain to their own specific duties. For example, a "PCI admin" could be authorized to work only with the virtual servers within the PCI cardholder data environment.

Best Practice 4: Secondary Approval ("2-Person Rule")

Another risk encompassing unrestricted privileged admin access is accidental mistakes that expose data to theft or destruction. One of the best practices to reduce this risk is to

Multi-Cloud Deployment Management

Financial industry is still in the early stages of cloud adoption with 61% developing a cloud strategy – *Cloud Security Alliance*

add a secondary level of approval for executing sensitive actions. For example, a junior IT operator would be prohibited from performing potential risky actions, like shutting down a production virtual server without approval from a more senior employee. Secondary approval is essentially the "two-person rule," which is based on the adage "trust, but verify." This has been applied for years in environments where privileged users' actions could result in significant damage. This simple, yet often overlooked practice, would have prevented the admin mistake that caused the Amazon Web Services S3 outage in February 2017.

Best Practice 5: Two-Factor Authentication (2FA)
Authentication is the process of validating that a login request originated with someone who is indeed authorized to use the account. Single-factor authentication has proven inadequate against the modern tactics of increasingly sophisticated hackers. Passwords can be guessed or obtained via session hijacking and key loggers on client PCs. They can also be shared improperly, such as when Edward Snowden's colleagues gave him their admin account passwords and he used them to collect thousands of confidential documents. 2FA is an authentication method that is more robust than a simple username and password. This best practice makes it infinitely harder to misuse accounts, because it requires two different identification methods to verify a person's login, for example, a password and a fingerprint.

Best Practice 6: Audit Quality Logging, Alerting, and Reporting
If an issue arises during data center operations, detailed logs are the first tools required to troubleshoot the problem. These logs should be examined forensically to determine exactly who did what to which workloads and when. Best practices include continuous admin activity logging that provides a complete audit trail, both for troubleshooting and for compliance and security controls. It also sends alerts on suspicious or abnormal admin activity, and activity reports on demand.

Best Practice 7: Data Geo-fencing
A critical best practice in today's multi-cloud world is having the ability to segment data and set when and where specific virtual workloads can run. With a wide range of local, national, and global regulatory compliance mandates, geo-fencing data ensures that it can be managed according to specific compliance rules, as well as according to risk classifications and levels of confidentiality. So, for example, German workloads can only run on German hosts, classified data can only run on classified hosts, and virtual workloads with intellectual property can only run within an organization's four walls. With proper geo-fencing controls in place, if a sensitive virtual workload is copied or removed from its defined location, it will not run at all, and the data cannot be decrypted on untrusted hosts.

Best Practice 8: Data Classification and Identification Tagging
This best practice supports data geo-fencing by providing functionality that digitally tags workloads to classify them and then set data policies by geographic region, regulatory compliance mandate, risk classification, and levels of confidentiality. It also allows easy policy changes, avoids the need to redo entire asset inventories, and ensures policy enforcement for data access, encryption, and key management.

The HyTrust Security Policy Framework – Powered by Intel

All of these eight best practices are available on the HyTrust Security Policy Framework. The platform includes DataControl, CloudControl, and BoundaryControl.

- **HyTrust DataControl** offers powerful data-at-rest encryption with integrated key management to secure virtual workloads and their data throughout their lifecycle. It's easy to deploy and manage and can run in any virtualized or cloud environment. With low-latency encryption accelerated by Intel AES-NI, the performance hit is negligible. HyTrust

Financial Institutions Face Multiple Compliance Regulations

Financial services organizations cite avoiding data breaches as their primary mandate, with banking compliance becoming their second most important driver – *SANS institute*

"The average cost for organizations that experience non-compliance related problems is nearly $9.4 million." – *Ponemon Institute's "True Cost of Compliance Report"*

48% of financial services firms expressed concern about understanding and complying with U.S. laws and regulations that impact on their business – *"Duff & Phelps Global Enforcement Review 2017"*

31% expected cybersecurity to be the top priority for regulators in 2017 versus just 19% in 2016 – *"Duff & Phelps Global Enforcement Review 2017"*

DataControl simplifies the process of encryption and key management but scales to enterprise-level performance.

- **HyTrust CloudControl** sets and enforces security policies and automates compliance requirements mandated by a broad range of government and industry standards on a full range of cloud deployment configurations. With automated compliance templates, 2FA, RBAC, secondary approval workflows and audit-quality logs, HyTrust CloudControl hardens virtualized and cloud environments for even the most sensitive industries and workloads.
- **HyTrust BoundaryControl** enables admins to set policies via tagging and identification, so that workloads only run on proven, trusted hosts that are physically located within the defined parameters. The product of over eight years of joint R&D work, HyTrust BoundaryControl leverages Intel® Trusted Execution Technology (Intel TXT), taking security to the hardware level. Intel TXT provides processor level-attestation of the hardware, BIOS, and hypervisor, allowing sensitive workloads to run only on trusted platforms. Users can also assign labels that bind workloads to predefined locations—if the workload is moved outside of this location it simply will not run. Moreover, encryption policies can be applied to ensure data is never decrypted outside of defined parameters.

With these essential cybersecurity capabilities, the HyTrust Workload Security Platform delivers critical cybersecurity best practices to financial services organizations that strengthen their data security and regulatory compliance—wherever data resides.

Strong Encryption
Only 42% of financial services firms have implemented data encryption solutions for the cloud – *Cloud Security Alliance*

Strong Key Management
61% of financial services firms said ownership of encryption keys is a concern – *Cloud Security Alliance*

To learn more about HyTrust products and services, visit:

www.hytrust.com/products/

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
1-844-681-8100 (US)
1-650-681-8100 (Intl.)

20171017-0026

Addendum: Financial Services Compliance Regulations

The world of financial services regulation is a labyrinth, to say the least. The myriad of ever-changing laws and regulatory rules that financial organizations must comply with can be confusing. Here are the most important compliance regulations that oversee cybersecurity in the financial services industry.

Agency	Description	Impacts	Policy Examples	Penalties
General Data Protection Regulation (GDPR)	Strict rules created by the European Union states to protect EU citizens; goes into effect May 25, 2018	Applies to every organization in every country that handles EU citizens' data	Organizations must know where their data is at all times, understand how 3rd parties use the data, and minimize access to data	As much as 4% of annual global revenue
Payment Card Industry Data Security Standard (PCI DSS)	A security standard for organizations that handle payment cards (debit, credit)	Any organization that stores, processes, or transmits payment card data	Organizations must protect all data in the cloud; have segmented views of PII data across multiple cloud apps and on-premises; make compliance updates while executing system modifications	Monthly fines from $5,000 to $100,000; loss of ability to accept cards
Federal Deposit Insurance Corporation (FDIC)	Supports standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information	Insured banks that handle savings accounts, checking accounts, NOW accounts, MMDAs and CDs	Organizations must design information security programs to control risks, commensurate with information sensitivity, as well as the complexity and scope of the institution's activities	Civil financial penalties against banks and individuals for certain violations; directors can be held personally liable; requests for damages by adversely affected parties; demands for corrective actions
Securities and Exchange Commission (SEC)	Oversees Administers the Safeguards Rule that requires all registered entities to protect against any anticipated threats to customers' PII	SEC registered broker-dealers and investment advisors who store sensitive client data	Organizations must ensure security and confidentiality of customer records; protect against anticipated threats or hazards to the security or integrity of customer PII	Financial fines; business censures and cease and desist orders; firing of responsible parties
Financial Industry Regulatory Authority (FINRA)	Private non-governmental organization that regulates members, including the deployment of cybersecurity programs	Member brokerage firms, advisors, and exchange markets	Organizations must have risk assessment, technical controls, and response plans	Financial fines, customer financial restitution, censure, and suspension of FINRA membership
Federal Financial Institutions Examination Council (FFIEC)	Interagency body of U.S. government comprised of several financial regulatory agencies, which prescribe uniform principles, standards, and report forms for federal inspection of financial institutions	All U.S. financial institutions	Organizations must follow guidelines on inherent risk profiles and cybersecurity maturity levels, including how susceptible they are to cyber attacks, and the strength of their cybersecurity programs	Supervisory or enforcement actions

Addendum: Financial Services Compliance Regulations (Continued)

Agency	Description	Impacts	Policy Examples	Penalties
Sarbanes-Oxley Act (SOX)	Mandates new standards for financial reporting, including how financial data is managed throughout organizations	All public companies and accounting firms	Organizations must safeguard to secure data integrity, and identify all data security controls	Heavy fines and/or jail time for C-level executives
Gramm-Leach-Bliley Act (GLBA)	Oversees Privacy Rule protecting consumers' financial privacy, and Safeguards Rule that requires organizations to implement security programs to protect PII	All financial institutions	Organizations must regulate the collection, use, and disclosure of PII, and provide opt-out options for customers	Varies depending on the authorizing statute of the agency that brings the enforcement action
Dodd-Frank Wall Street Reform	Indirectly impacts the cybersecurity requirement, specifically regarding enforcement of the GLBA Privacy Rule	All financial institutions	See GLBA above	See GLBA above
Federal Trade Commission (FTC)	Regulates company's cybersecurity practices under its unfair and deceptive acts or practices provisions; and enforces Dodd-Frank's GLBA Privacy Rule	All financial institutions	See GLBA above	See GLBA above
New York Department of Financial Services (NYDFS)	Updated New York State cybersecurity regulations (August 2017) to ensure soundness of New York's financial services industry	Any person operating under or required to operate under the Banking Law, Insurance Law, or Financial Services Law in the state of New York	Organizations must establish and maintain documented cybersecurity policies designed to protect consumers' PII; policies must address security best practices, including access controls, data privacy, data encryption, and multi-factor authentication	Individual civil and criminal penalties