sysdig

BRIEF

6 Key Challenges for CISOs in Financial Services

Challenges Everywhere, All At Once

Organizations in all industries have faced a cybercrime goldrush in recent years, and unsurprisingly, financial services providers have been a prime target. Ransomware attacks alone affected **74% of global financial institutions in 2021–2022** and the average cost of a data breach in the sector hit **$5.72 million**.

Financial details are highly prized and offer even inexperienced hackers an opportunity to make a quick buck: credit card numbers, for instance, can be easily sold for $30 a go. Increasingly, attackers are exploiting vulnerabilities in cloud security architectures to grab such valuable information, with Sysdig's latest research finding that 65% of cloud attacks now target financial services companies and telcos.

At the same time, financial service providers must stay compliant with constantly changing cybersecurity standards in one of the most heavily regulated industries in the world. As cloud migration in the sector gathers pace, security leaders face a balancing act. How do you deal with complex cloud security and compliance challenges, without slowing down the development of products that deliver growth?

Let's look at the key challenges you're facing today, and how to navigate them.

01 Defending Against Burgeoning Cyber Attacks

Cloud momentum is accelerating: 54% of financial institutions expect to shift **at least half of their workloads to the public cloud over the next 5 years**. Building applications in the cloud improves agility and speed, but it's also creating something of a free-for-all among developers who are now able to deploy containerized microservices at the click of a button. With escalating volumes of assets and activity to track, critical vulnerabilities and misconfigurations can easily be missed.

Threats are emerging on multiple fronts. Software supply chain attacks, in which malicious elements are introduced via common libraries or tools used in your code, are increasing exponentially at **4-5 times per year**. Open Banking, while creating exciting opportunities for innovation, is also generating new risks, with attacks on financial web Applications and APIs surging by **3.5 times year-on-year in 2022**.

To deal with these risks, your organization needs a security solution built for the dynamic nature of the cloud: a single platform combining workload protection, cloud security posture management (CSPM), and real-time threat detection allowing you to respond to incidents without delay.

x3.5

rise in web application and API attacks in the financial services sector in 2022 [1]

Takeaway: The cloud has changed the nature of app development – and security is feeling the impact. Closing visibility gaps and securing the devops workflow must be a priority.

[1] *Source:* **InfoSecurity**

02 Securing Your Customers, Without Compromising Their Experience

Speed is of the essence in the competitive world of financial services. A new generation of fintechs has set the benchmark for feature-rich, customer-centric experiences, and the pressure is on providers to stay competitive by bringing product enhancements to market, fast.

Digital transformation programs are key to delivering to these goals. But overly hasty cloud migration can quickly create security holes – and customers expect the highest standards of security and privacy when it comes to their finances. The challenge is to safeguard data and stay compliant without slowing

Takeaway: Cloud agility and automation are critical to innovating at speed – but trust must be protected.

your development team down. Modernizing apps with AI, cloud technology and automation is critical to build seamless customer experiences and release them at pace. But this must be done in conjunction with a careful risk management strategy, to protect your company's reputation and maintain trust.

03 Safely Migrating From Legacy Tech

The rush to digitization during COVID saw many businesses adopt short-term measures to adapt to an unprecedented situation. Unfortunately, that only added to the pile of point solutions and technical debt hampering their security, agility and ability to innovate. The more unchecked debt grows over time, the more difficult it can be to adapt and extend – and the more of your company's development budget it swallows up. According to **McKinsey**, more than 20% of technical budget ostensibly dedicated to new products is diverted to resolving issues related to tech debt.

A well-planned cloud migration strategy can help you address the performance issues of aging systems and reverse technical debt at a prudent and realistic pace. But since cloud and containers bring their own unique security challenges, seek solutions that are built for the cloud's dynamic attack surface and help you prioritize the most critical risks.

20%

of technical budget ostensibly dedicated to new products is diverted to resolving issues related to tech debt [2]

Takeaway: Look to solutions that let you safely retain legacy systems, while assisting gradual migration to the cloud.

> "We need to be able to count on the security and the integrity of containers that may be online for a few seconds, maybe a few weeks, before they disappear."

worldpay from FIS

Natnael Teferi
Lead DevSecOps Cloud Security Architect, Worldpay

[2] *Source:* **McKinsey**

04 Staying Compliant with Evolving Regulations

As financial regulations increase in strength and scope, managing compliance is becoming increasingly complex. CISOs are faced with a huge volume of standards with which to keep track, some of which are optional, some compulsory, some that vary by region, and many that overlap. With data security, protection, and resilience a focus, regulators are requiring these to be baked into processes and practices, from design right through the lifecycle. And non-compliance is costly: in 2022, fines for violating financial services regulations totaled **$4.17 billion**.

However, compliance doesn't necessarily equate to security. The goal is to foster a positive security culture across your organization, supported by the right policies, processes, and technology. This will encourage everyone to behave more safely and reduce the chances of human error that can result not just in non-compliance, but harm to your business.

Takeaway: Compliance starts with people and building a culture that makes cyber security everyone's business.

05 Tackling the Cyber Risks of Geopolitical Conflict

Geopolitical conflict goes hand-in-hand with a surge in cybercrime of a particularly dangerous sort. Such attacks can be highly sophisticated and their proponents well funded by unscrupulous regimes seeking to compensate for revenue loss from economic sanctions or even to destabilize entire industries or regions. In response to the heightened global threat, your peers are ramping up security: over a quarter of organizations in North America and EMEA took **some kind of cybersecurity action** following Russia's invasion of Ukraine.

Security leaders should assess the exposure of systems, people, and data in countries subject to attack, dial up security, and ensure a robust incident response plan is in place. Consider also strengthening identity and access management, and educating employees on detecting and mitigating phishing and social engineering attacks, to prevent bad actors from infiltrating your systems via stolen account credentials.

Takeaway: Understand the security impact of global events and raise awareness among the organization as a whole.

06 Dealing With the Cybersecurity Talent Shortage

Good tech talent is increasingly hard to find. Leaders are struggling to recruit amid the global shortage of cybersecurity expertise, with over **3.5 million global cybersecurity positions** remaining open at the end of Q1 2022. That not only impacts your company's ability to keep up with rising threats, but also puts more pressure on your organization's bottom line as salaries escalate in consequence.

As businesses seek to 'shift left' and move tasks earlier in the development process, the burden of security is falling disproportionately on developers, who may not possess the appropriate expertise. The right technology solution can mitigate this by simplifying the task of building security into applications, for example by providing a single, shared source of insight, automating routine tasks, and helping developers prioritize the high volumes of alerts they have to deal with.

Takeaway: Seek technology that allows non-experts to do their bit to ensure security with minimal effort.

Securing Financial Services at Cloud Speed

Your organization faces challenges on multiple fronts: engaging the next generation of financial services customers while keeping your systems compliant and secure.

Cloud migration is critical for accelerating speed to market, but opens up the risk of unknowns. To safely leverage the cloud's agility and speed, a robust cloud-centric security architecture is essential.

But, security starts with people. A strong security culture, in which everyone has a role, will do most to establish long-term resilience for your business. Encouraging cyber-safe behavior across all teams will provide the greatest protection for your organization, and avoid it becoming the next big data breach headline.

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

Discover five things CISOs in banking and financial services can do to make containers secure and compliant.

READY TO PUT CLOUD SECURITY FIRST? →