

Institutionalizing Software Security

Financial Services: A case study in risk management

Companies must both innovate and “inoculate.”

A holistic view of security with a view to the future.

Security is a competitive advantage.

For decades technology has been an obvious key to competitive advantage across nearly every industry. Fact: companies must innovate in order to survive. But there is another fact: innovations invite vulnerability. While software programmers churn out millions of lines of code every year they are not just racing against the competition; they are also racing against a new breed of cyber criminals. The rules of the game are hanging. The new key to survival is security.

Customer trust cannot be undervalued.

Customer trust is possibly the most valuable asset for any company. In order to make it in this climate companies must now innovate *and* “inoculate” in equal measure to implement novel technology while developing tools and processes to protect that technology. This shift toward risk management requires a culture change; those companies who adapt have the true competitive advantage.

Is your company’s investment in risk management adequate?

As consumers in the global marketplace go about their daily business, utilizing code-driven technology, they leave a trail of potentially vulnerable private and sensitive information. Every time they slip a card into an ATM machine or log on to a banking website a vote of confidence is being placed in the security systems behind their transaction. But is that trust earned? Many companies are enjoying high levels of consumer confidence without having kept pace with the changing environment of network safety and new vulnerabilities that seem to constantly develop. They have not adequately invested in the level of risk management now associated with handling this sensitive information.

Protection against external forces is not enough.

Hacking is not a hobby any more; it’s a highly skilled profession. Cyber criminals are well-funded and well-



equipped with sophisticated, automated tools. It’s their full-time, lucrative occupation to find and exploit security vulnerabilities at the expense of consumers and companies alike. It’s not just a matter of external firewalls and other similar types of protection either. In a recent survey 78% of IT executives reported insider breaches¹.

Still, it’s not surprising that some firms remain a bit too complacent about security at the same time demands for anywhere, anytime access to their enterprise are growing exponentially. Companies are under constant pressure to remain extraordinarily nimble—required to quickly innovate, institute and adopt new software technologies—if they are to be successful.

Financial services company makes security a key priority.

One international financial services company has made security a cornerstone of its software strategy. With assets in the trillions of dollars this company is a leading provider of mutual funds, workplace retirement savings plans and a spectrum of other financial services including brokerage, estate planning, wealth management and more. Millions of individuals have entrusted their retirement planning, brokerage or human resources benefits with one of the firm’s many divisions. Determined to keep its customers’ trust the company has made software security a key development priority.

Technology and innovation create competitive advantage.

The company remains agile by investing more than 15% of its annual revenues into identifying technologies and tools to benefit their customers, agents and employees. With a quarter of the workforce and significant budget devoted to IT the company views innovation as a key competitive advantage, yet also recognizes the risks associated with all new technology. Their head of security has commented, “*What sets us apart is that we place enormous value on the security of the firm’s and our customers’ data.*”

State-of-the-art tools are only one factor for security.

Concern for its customers and dedication to top-flight security led the firm to seek the help of Cigital, whose

professionals have over a decade of software security and quality engagements for world-class clients. The financial services firm had already evaluated a number of automated code-scanning tools designed to detect certain software risks and chosen Fortify Software based on the performance of their application protection products. State-of-the-art tools, however, are only one factor affecting the ability of any firm to reduce the risk of software vulnerabilities.

Real-world project and risk management expertise needed.

Cigital was apprised by the client that the main intention was to do the job right from the start. They had realized early on that the biggest challenge in institutionalizing software security is not the technology—but the culture change required. The expertise of Cigital was intended to guide them around the pitfalls of a major change by providing experts with the most relevant, proven experience. Company management understood the need, not only for a comprehensive program designed by professionals with real-world project and risk management success, but for support from the top level executive suite. Securing the support of senior executives would allow them to minimize future exposure to breaches and assure compliance with regulatory mandates. The initiative necessitated a holistic and systemic view of security.

Custom-crafted rules to streamline the process.

First, Cigital and the client worked together to devise an algorithm that determined specific software risk profiles, allowing them to focus on the highest risk applications. Next, the Fortify software was fine-tuned with customized rule sets to pin-point those vulnerabilities that mattered most to the company. Because Cigital custom-crafted rules unique to the company's needs the code review tools were made more reliable and efficient. Instead of being inundated by thousands of findings, programmers could begin with a much smaller set of targeted results. And with Cigital's custom rules results included corporate standards violations in the code.

A company-wide program starting with senior management.

The combination of targeted risk profiles and finely-tuned automated scanning created a manageable workload for those responsible for software security within the firm. The client reinforced their investment by impressing upon its developers/programmers the importance of proactive security. Cigital helped the firm deploy a comprehensive program including hosted on-site tech events for their IT community and other incentives involving Human Resources and Senior Management.

Software security an integral part of the development process.

Cigital and the client are midway through a multi-year process that continues to receive support and commitment from the most senior levels of the firm and their development community alike. With this mandate, software security has become an integral part of the client's software development process—not an afterthought to bringing new applications online. The firm has acquired invaluable, repeatable processes, tools and methodologies that can be scaled to include the majority of software developed within the firm. Today these processes can quantify security and measure progress of software throughout the development process. New best practices and security guidelines are now being established based on these core findings. The company has created a successful approach to managing software risk.

Razor-sharp focus on security setting new standards.

Security has always been of primary concern to the banking and finance industries. But the threat to institutions has grown more insidious and global in scope. Today's criminals operate from anywhere on the globe with complete anonymity, armed with *the latest* tools and technologies. Securing the integrity, availability and confidentiality of information requires an arsenal of software best-practices. Chief Information Security Officers (CISOs) are the new keepers of the keys, joining CIOs and CFOs as critical functions of any healthy company. With its razor-sharp focus on guarding customer data, this financial services industry leader is setting the standard for institutionalizing the practice of software security.

About Cigital

The growing demand for ubiquitous connectivity throughout the enterprise, for universal access to information and communications creates new, unforeseen vulnerabilities. Founded in 1992, Cigital is a leading consulting firm specializing in software security and quality. Our experience has demonstrated that the right solutions are built in, not "bolted-on."

Cigital's experts mitigate software-induced business risks and identify performance issues that have business consequences. We assure the reliable delivery and deployment of software that organizations build, buy and integrate. Cigital is headquartered near Washington, D.C. with offices in Boston, New York and Los Angeles.



Software confidence. Achieved.