MAINTAINING TRUST

Financial Services That Are Secure, Consistent, and Responsive

"Cyber-confidence is crucial for finance. Consistency between security and threat is a key factor in Reputation and Customer Trust."

Stéphane Nappo, IBFS Global Chief Information Security Officer & Board Advisor, Paris, France

REGULATION AND BANKS

The financial industry is experiencing a significant challenge when it comes to maintaining and establishing trust in its relationships with clients. Customers battered by the constant barrage of publicized data incursions and security breaches are highly sensitized to those signs in their own dealings. They find it difficult to accept any disruption in either their business or their personal financial activities and are easily frightened away from organizations that they perceive as risky.

While the challenges facing organizations that help customers to maintain and manage wealth are volatile overall, the problem becomes especially significant for those institutions that are more mature and that fall within the regulated environments. This combination changes the burden of operational activity and also creates an underlying perception to the public that they might be less innovative than the newer, more Internet-savvy organizations.

The recent changes in the regulations that govern financial institutions have been eased to remove some of the burden from the smaller and midsize financial groups. This has been touted as a victory for the reduction in government interference and an incentive for smaller companies to expand their business and better serve consumers.

However, this has put the larger organizations at a disadvantage. Those institutions that are still required by law to conform to stringent rules and controls now have a relatively more substantial burden of expense and policy that increases the cost and complexity of doing business. That difference alters how they appear to the public, and ultimately, how well they acquire and maintain their market share.

This situation creates two effects in the overall business environment, one which is that smaller banks now are freer to nibble away at the established customer base of their more restricted competitors. Since the acquisition and maintenance of customers is a substantial part of any longevity plan, the investment that the more established organizations have in their customer base is a prime area of contention.

The financial institutions that are energized to actively solicit customers by their escape from the full spectrum of regulation are doing so without the same set of guidelines that the mature financial environment requires. Reporting requirements on any data breach are less onerous, procedures that must be followed before issuing loans are less stringent, and so on. These are just a few of the differences that the more mature financial organization has to address while its far more agile competitor is more open to innovative and rapid offerings.

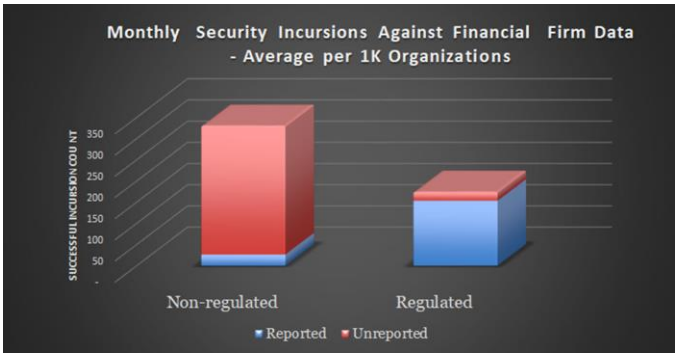
SECURITY AS THE NUMBER ONE FOCUS

In the market today, security is the number one requirement and focus point. It is the issue that concerns most consumers and organizations that do business, especially those that conduct the majority of their

activities via the Internet. The higher requirements of reporting and transparency on data breaches for the regulated financial institutions means that their data incursions and the associated impact are more evident to the public.

Danger and impact make better press. So announced incursions, failures, etc., are pushed through the escalating business world with a disproportionate amount of attention. Any incident is made more visible through the public appetite for escalating news and emotional analysis. High levels of awareness on social media and press around a problem can make an organization appear both less secure and riskier to both current, and possible future, customers.

In a recent Solitaire Interglobal Ltd. (SIL) study, a broad spectrum of effects on the financial industry was examined. Looking at both regulated and unregulated financial services organizations, the analysis highlighted significant patterns that are shaping the market. One of these aspects can be seen in the following chart that shows the number of announced and unannounced security incursions, split by regulatory oversight classification.



The influence of maturity and regulation compliance can be seen in the overall incursions for the different groups, but the requirements to report more of the incursions to oversight bodies generates an appearance of more risk for those organizations. This is both misleading and difficult to counter.

The additional burden of process compliance within the regulatory structure also affects the agility of any organization offering financial services on the web. With a lighter load of regulation, the smaller organizations demonstrate a faster time to market and more agile response to market conditions. In many cases, this is impossible for a regulated institution to match, since the checkpoints that need to be performed have built-in timing and risk mitigation safeguards.

When the contributing organizations included in the previous chart were queried as to the amount of time spent between primary development and regulatory compliance efforts, the breakdown in agility shows that a significant portion of the responsiveness on the part of the more mature institutions is spent in meeting the requirements of their oversight rules.

Both of these are areas that will provide a false picture to customers looking to either find a financial institution or being wooed away from their existing one. All that a less regulated organization has to do is point to the required reporting of data breaches that their competitor has filed and highlight that their own organization has not had to submit such breach information. There is no need to say that the poaching organization has not been breached or is secure, the campaign merely uses press and publication to do its marketing by implication.

A similar pattern can be used to tout the agility and innovation of the less regulated bank. By pointing out faster releases and time-to-market intervals, the more nimble organization appeals to consumers' idea of what the Internet should be and how business should be conducted over it. It falsely identifies the faster organization as more supportive and higher quality, without presenting a full picture of the relative

values. This aggressive and predatory marketing is on the rise.The market seizes on this type of data and leverages the information into extremely effective campaigns. An examination of the last eight months shows the increase of this approach in the market, with significant escalation marked by the easing of regulations established by the Dodd–Frank Wall Street Reform and Consumer Protection Act.

There are few ways to combat this type of ambient marketing. In the competitive world of Internet banking and customers that are increasingly savvy about the use of the web to maintain their business, it's specious to fight against what is commonly known knowledge. Instead, it becomes even more critical for the mature financial organization to have a strong foundation in both security and agility.

If the underlying infrastructure provides foundational security that is far better than its competition, the burden of reporting and publicizing security breaches that are being mandated under regulation can be met in accordance with the law and still minimized with a more secure base. Of course, the effectiveness of the foundation is something that can be either improved or degraded based on the individual financial institution's adherence to both best practices and comprehensive security postures. However, the underlying foundation is a critical factor in leveling the playing field when it comes to presenting a more secure picture to customers.

A similar situation can be found when examining a competitive picture of agility. If a financial institution's information technology is built on a platform that carries advantages in deployment, part of the disadvantage of regulatory burdens of process and time can be offset.

In each of these cases, it is essential to present a balanced picture to current and potential customers. The speed of innovation and the protection of customer data are crucial, but they are not the only differentiators that can be presented to the customer.

Important differences in metrics that are continually ranked among the top ten factors for financial customer satisfaction can be included. These are consistency and quality of service.

This is where the mature financial organization can tune its marketing to counteract some of the disadvantages of the increased regulatory burden. By taking this view, customers can be reminded of the value of consistent product releases, dependable runtimes, and high levels of availability. This speaks to the quality of service provided by the institution.

Only with a comprehensive and robust picture can a regulated financial organization compete with the almost "Wild West" days of the unregulated competitors. By showing the value of a stable, consistent, and safe environment for banking, they can keep existing customers and offer a safe haven for those who have been stressed by their less-regulated cousins.

IBM LINUXONE AND REGULATED BANKS

IBM LinuxONE is a significant component in constructing a foundation for quality. It addresses the critical areas of success in the burgeoning market of security, agility, and quality of delivery that enables organizations to respond to the challenges that are demonstrated every day in cyberspace.

Speed and safety are strongly affected by the LinuxONE solution. Offsetting regulatory burdens with a platform that carries embedded advantages for security and agility is exceptionally beneficial. The differences in this area are significant with speed *savings of up to 60%* or more.

Security is where the LinuxONE option makes the most significant difference. Hackers are far less likely to be able to breach the protections that are necessary for digital inventory when the foundational

cybersecurity has a more stringent starting point. In fact, LinuxONE implementations report *less than 0.01%* of successful security incursions per 1000 deployed applications than other architectures.

In the volatile cyberbusiness world, confidence in the organizations that hold the cornerstone control of finances is the most sensitive and fragile. Protecting that trust outweighs other concerns, but unless a mature regulated financial organization can present a full picture of the benefits that come with their offerings, the less-regulated and more predatory competitors will continue to make inroads on the market.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) has been gathering data on market evolution and production behavior for over 40 years. Supporting more than 6,000 clients and performing over 100M predictive models each year, SIL has also run the Global Security watch for the last 22 years. That member service has allowed SIL to build a repository that exceeds 550 PB of data at a very granular level. That data is mined every hour for trends, comparisons, and threshold that help organizations succeed.

ATTRIBUTIONS AND DISCLAIMERS

41019641USEN-00