

From Risk to Reward: How to Profit from IT Security

Competitive pressures have slowly been forcing financial services institutions to manage security issues proactively rather than reactively even as security threats and compliance demands multiply and grow in complexity. An increase in data leakage, for instance, is forcing institutions to employ new strategies even as the challenge remains defining and implementing the security measures that can deliver business improvements and increased profit. We ask industry leaders to tell us what financial institutions need to do this year.

Alexander C. Tabb

Partner, Crisis & Continuity Services
TABB GROUP

Alex, we've seen the headlines, but in your view, what are the top threats this year? What's on the horizon?

While it is obviously impossible to predict the future, the most pressing, demanding security vulnerabilities surround the security and protection of critical customer data. Unfortunately, the financial services industry is particularly susceptible to these issues, as the nature of this data in question is often very sensitive. Compromised systems and unauthorized access to confidential customer data can jeopardize any institution, creating significant liabilities and, a critical issue for shareholders, damaging a firm's valuable reputation.

Overall, how well are financial institutions doing in shoring up their security? Any surprises?

Overall, the sector is taking the threat very seriously and investing significant resources in trying to 'keep up with the Joneses.' Unfortunately, information security is an evolutionary process driven by the unfortunate experiences of other institutions. As such, firms have to remain vigilant at all times.





Tabb

How will success be defined in 2007 and what do you see as best strategy to achieving this?

Success? It's measured by a 'lack of failure,' a paradigm that simply has to change if the sector is to remain vigilant. We believe that for a firm to be successful it must harness the intellectual capital it has developed over time, empowering them to create new, cost effective and innovative solutions.

In 15 words or less, tell us what a financial firm should definitely not do when making an IT investment.

15 words? Look to the future when developing and implementing new security solutions, not to the past.

Sathvik Krishnamurthy

President and CEO
VOLTAGE SECURITY



Krishnamurthy

Sathvik, in your view, what are the top threats this year?

The top threat this year continues to be brand erosion through data breach disclosure laws associated with lost files, infiltrated emails, and databases containing personal information such as social security numbers and credit card numbers. A close second is the threat to loss of intellectual property and other trade secrets. Enterprises are losing control of this information as it leaves the organization through email, removable media, instant messaging and other peer-to-peer networks.

Overall, how well are financial institutions doing in shoring up their security?

In many ways they are just at the beginning, as they shift their focus from infrastructure protection to protecting the data itself. Financial institutions are working aggressively to plug the gaping holes. In most cases, they have appropriately prioritized their threats and addressed the high priorities first. The 'containers and pipes' that are used to store and transport sensitive information tend to be the first threats that are addressed, such as laptops, SAN/NAS and SSL. However, the next wave of security that we are increasingly seeing as a top priority for financial institutions is ensuring protection of the data itself via encryption technology such as Voltage's IBE and Key Management.

How does your firm help FIs with their compliance and security efforts?

Voltage Security delivers the ability to implement and enforce protection of sensitive data persistently – at its source. For financial institutions, this means drastically reducing risk and complexity. Voltage Security offers data-centric protection for email, files, test data and applications. This is all backed by a highly efficient key management and auditing platform to help financial institutions move patchwork encryption programs to a central, well governed data protection program.



Horvath



Prylowski



In 15 words or less, tell us what a financial firm should definitely not do when making an IT investment.

Lose sight of business process requirements by getting lost in technical features.

Mark Horvath

*Director of Engineering,
Worldwide Financial Services*
MICROSOFT

We've seen the headlines, but in your view, what are the top threats this year? What's on the horizon?

As always, the basics matter. Patch management, desktop updates, and virus control, while seeming so '2004,' are still big issues for a majority of companies that have not completed their upgrades and investments in their IT infrastructure. Fortunately, these companies are becoming a smaller portion of the overall FSI community. For those that have completed these measures, the prospects look a lot better. They are in the process of addressing larger issues like phishing and identity management. Phishing remains a constant problem for the industry even as a lot of progress has been made with advances in Identity Management technology. For fiscal year 2008, look for major FSIs to begin rolling out the next generation of IDM software, allowing not just customers to identify themselves to their FSIs, but allowing the FSIs to identify themselves to their customers.

How well are financial institutions doing overall in shoring up their security? Any surprises?

Building on the success of earlier years, FSIs are doing quite a bit better in the security space. In one recent survey (Internet Crime Complaint Center and *U.S. News and World Report*), online auction fraud has far surpassed identity theft as the number one reported consumer crime. This is good in that it highlights the progress companies have made on the issue, but it also shows that criminals will always adapt to the weakest point in the security perimeter. An active, managed security profile is the key thing for FSIs to maintain if they want to keep out of the headlines.

How will success be defined in 2007 and what do you see as best strategy to achieving this?

Security success, at least for FSIs, is all about two things: the low numbers of incidents that affect their clients (phishing, ID theft, hacking, and information theft) and staying out of the headlines, at least on security and regulatory compliance. Again, the best defense is to continue to invest in the security infrastructure and to establish a coherent, actively managed security plan. A security response plan is also important as FSIs are always in a defensive mode with respect to security. The threats change and adapt. FSIs need to keep their guard up, to continue to work their defense, and to keep their eyes on the ball.

Mark, tell us what a financial firm should definitely not do when making an IT investment.

They should not make the mistake of thinking of security as 'solved.' The next threat is always right around the corner, and the first ones to get hit are the ones that think the battle is over.

Tony Prylowski

Chief Executive Officer
EXSAFE, AN ROISOFT COMPANY

Tony, what do you see as the top threats this year?

There has never been a time when the threat of information leakage was greater. Whether it is from bad practices, inadvertent employee errors or malicious actions, it can be alarming the kind of critical data that are leaving the safe confines of financial services firms. Not only is personal customer information and intellectual property at risk, but so is internal employee information. For example, we have observed on numerous occasions employee salary information being freely circulated in unprotected spreadsheets.

How well are financial institutions doing in shoring up their security?

One area that needs focus is mobile computing. One of the biggest contributors to data loss is the ubiquitous laptop. Over half of all computers sold now are laptops and senior executives at financial services firms are some of the biggest users of portable computers. This is why it is so critical to secure the Excel, Word, and PowerPoint files residing on these machines. While Microsoft provides their Information Rights Management tools that can prevent printing, copying and pasting, our ExSafe security framework takes these basic security steps to a whole other level.

How does your firm help FIs with their compliance and security efforts?

Auditors and compliance officers love to see audit trails and we satisfy this desire with end-to-end auditing capabilities. Every change – and every attempt to change an ExSafe-protected document – is audited, so from a change management perspective we provide a 360 degree view of the document. Additionally, we provide complete version control by saving every older version in an encrypted format. While users are traveling, ExSafe maintains all security and management controls while they work in an 'off-line' environment. They can still edit their ExSafe-protected documents and as soon as they reconnect to their network, we automatically synch their data.

And now, in 15 words or less, tell us what a financial firm should definitely not do when making an IT investment.

Information is Power, don't give it away freely, ignore its security at your peril.