



**Whitepaper:**  
**COMMUNITY BANKS:**  
**CONSIDER OUTSOURCED SECURITY SERVICES**

**866.333.2133**  
**[www.solutionary.com](http://www.solutionary.com)**



## COMMUNITY BANKS: CONSIDER OUTSOURCED SECURITY SERVICES

When Information Security Media group, publisher of BankInfoSecurity.com and CUInfoSecurity.com, conducted its *Banking Confidence Survey* at the end of 2008, 96% of respondents said the financial services industry had lost significant consumer confidence in the past year. This decline in confidence places pressure on financial institutions of all sizes, including community banks, which are quite possibly even less agile at dodging the arrows coming at banks from all directions. Reputations are being tarnished, data privacy is common conversation in lunch rooms and boardrooms, and community banks need solid options for doing more with less.



For community banks, Managed Security Service Providers (MSSPs) may be the best option for consideration. MSSPs can hit the ground running, stepping in to enhance existing security programs, strengthen processes, and improve data security and compliance with regulatory requirements.

Banking Priorities for 2009	
<ul style="list-style-type: none"><li>• Identity Theft</li><li>• Authentication</li><li>• Insider Fraud</li><li>• Web Security</li><li>• Messaging Security</li><li>• Data Loss Prevention</li></ul>	<ul style="list-style-type: none"><li>• Application Security</li><li>• Customer Trust</li><li>• PCI, GBLA, SOX</li><li>• Identity &amp; Access Management</li></ul>

\*Based on independent survey data and traffic patterns from BankInfoSecurity.com and CUInfoSecurity.com.

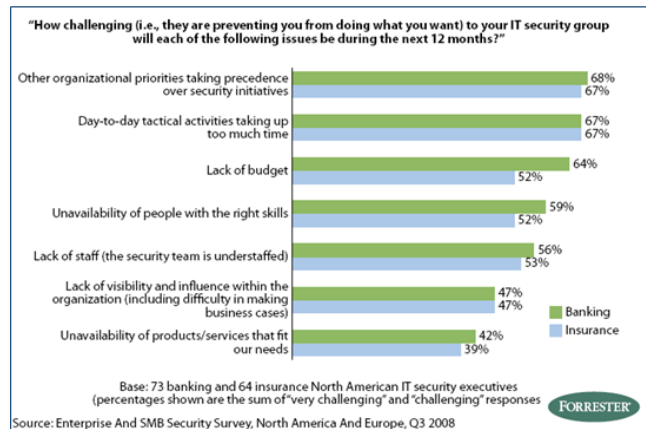
If there were just one area of focus, life would be simpler for community banks, but that just isn't the case. Competing priorities are pulling IT and security resources in myriad directions, challenging even the most process-driven banks to shudder with concern.

Just like large banks, community banks must have a variety of automated security measures in place to adequately defend against security threats and comply with standards and regulatory requirements such as GLBA, FFIEC, FTC, Red Flag and more. These mandates touch many parts of the infrastructure and impact the way community banks address:

- Network Intrusion Prevention
- Firewall Management and Monitoring
- Server Intrusion Prevention
- Event Log Monitoring, Analysis & Reporting
- Vulnerability Management

There are predictions of more frequent/detailed audits and reporting requirements focused on the banking industry.

There just are not enough resources in-house with the right skills and experience to tackle all that needs to be done. Community banks are not alone in their inability to allocate trained security resources for the focused initiatives core to a solid security program. As the table shows, **people** are the biggest challenge to IT security groups in financial services. All the above make outsourcing a solid value proposition that cannot be ignored.



A recent conversation with Forrester Research VP, Jonathan Penn, identified several key reasons outsourcing to an MSSP can make good business sense:

- **Skill set / competency.** Increasing, businesses recognize they lack in-house expertise to make smart buying decisions on certain security technologies – and then manage those technologies. Trained staff are not available to keep up with the evolving threat landscape and respond accordingly: changing firewall and IDS policies, updating anti-spam settings, perform vulnerability analysis and penetration testing, etc.

Banks also are recognizing that these are tasks they don't need or want to retain in-house, but are better left to experts for whom this is their business.

- **Simplicity.** Off-loading the operation of certain security processes or the management of certain security technology frees up the attention of security staff and managers to focus on more strategic issues. They no longer have to respond to every single security event or oversee time-intensive processes that can be operationalized and don't require an in depth understanding of their specific institution.

MSSPs provide faster time-to-production when introducing new security technology – both because of their expertise with the technology and how it's used, and also because they have designed their services to be as turnkey as possible. The faster clients are up and running on a new managed service, the more profitable it is for the MSSP and the faster the time-to-value for clients.

- **Cost savings.** MSSPs offer community banks solutions that are built to scale, and can operate systems and manage processes at far lower costs than smaller or medium sized banks can achieve. That savings is directly passed to the bank.

The cost of an MSS is typically less than hiring in-house, full-time security experts. For example, the savings of the initial setup of the hardware and software for an in-house solution versus that offered by an MSSP is as high as 93%. An MSS can reduce the institution's ongoing, annual costs of the same service by 63%. (For a detailed example of this analysis see the Cost Benefit Analysis at the end of this paper.)

- **Cost model.** Community banks (and they aren't alone) face significant capital expenditure pressures. The subscription and usage-based pricing of MSSPs is attractive because:
  - a. Costs are allocated to operational expenses, and
  - b. Pricing flexibility allows for adjustments to organizational changes.

There is no long-term lock-in on licensing or maintenance, and you tie ongoing costs directly to resources covered by the service (e.g., headcount, number of devices managed, etc.).

- **Knowledge base.** MSSPs have hundreds of clients, which gives them great insight into organizations of similar size/industry/geography/risk tolerance/etc.: what they are doing, how they are doing it, what it is costing, how many people they have doing it, and so on. MSSPs' analysis of their client base makes them a great knowledge source for benchmarking data, best practices, and emerging trends.

Of special interest for community banks, MSSPs may have unique insight on staffing allocations and reporting structure (banks tend to organize and operate their security programs quite differently from those of other industries), phishing trends, data breach or phishing incident response planning, and fraud trends.

Furthermore, many institutions, and well as their examiners, place significant value on having an independent third party, such as an MSSP, responsible for certain key security measures, and it can help address separation-of-duties issues community banks often face due to their limited staffing.

## **Conclusion**

Given the current economic and regulatory environment, community banks are under greater pressure than ever to do more with less. In many cases, community banks are finding that it is cost-prohibitive to implement and operate in-house many of the security measures required to keep the bank and its customers safe, as well as meet regulatory requirements. As a result, many community banks are finding that outsourcing some of these key security measures to an MSSP can be a sound business decision.

Cost Benefit Analysis: next page

# Cost Benefit Analysis

## Managed Security Services vs In-House Solutions

Cost Breakdown	Internal	Outsourced	Savings	%
<b>Capital Investment vs MSSP Initial Fee</b>				
Tools <sup>1</sup>	\$ 255,000			
SOC Infrastructure <sup>2</sup>	\$ 30,000			
MSSP Fees/Charges <sup>3</sup>		\$ 21,000		
<b>Total - Initial</b>	<b>\$ 285,000</b>	<b>\$ 21,000</b>	<b>\$ 264,000</b>	<b>93%</b>
<b>Annual/Ongoing Expenses</b>				
Resources (3 SOC Operators) <sup>4</sup>	\$ 243,750			
Management Costs <sup>5</sup>	\$ -			
Security Engineering Costs <sup>6</sup>	\$ 52,500			
Training <sup>7</sup>	\$ 15,000			
Tools, Maintenance <sup>8</sup>	\$ 54,000			
SOC Operating Expense <sup>9</sup>	\$ 6,200			
Depreciation and Amortization <sup>10</sup>	\$ 95,000	\$ 7,000		
MSSP Fees/Charges <sup>11</sup>		\$ 156,750		
<b>Total - Recurring</b>	<b>\$ 466,450</b>	<b>\$ 163,750</b>	<b>\$ 302,700</b>	<b>65%</b>

Save **93%** on capital investment towards tools and SOC infrastructure by selecting an MSSP.

Save **65%** on annual and recurring expenses by selecting an MSSP.

### How your savings stack up with an MSSP

- 1 Based on a conservative budget estimate of \$190,000 for SIM tool and \$65,000 for installation
- 2 Based on MSSP's client experience with a medium sized SIM and monitoring implementation
- 3 Represents hardware fees plus set-up fees
- 4 Average fully loaded compensation of \$65,000 plus 25% for benefits
- 5 Management costs not included. Realistically, client will require a SOC manager to handle operation or a dedicated person to assist with compliance reporting requirements.
- 6 Experience of an MSSP's clients who have implemented SIMs/IDS/IPS - ongoing security engineering costs above and beyond SOC resources (300 hours x \$175)
- 7 Training costs are based on estimate of two weeks of training per operator per year @ \$500 per day
- 8 Based on 20% of software costs and 10% of hardware costs
- 9 Miscellaneous expenses, primarily telecommunications
- 10 Based on total capital investment with a three year depreciation/amortization schedule
- 11 Annual MSSP fees based on monitoring/management for a three (3) year contract for eight (8) high end security devices, 50 servers with high priority alerting only, and 150 servers (SEIM)



## About Solutionary

Solutionary delivers exceptional information security and excellent customer service for clients seeking to improve data security and address compliance requirements.

Organizations world-wide depend on Solutionary's managed security platform, information security and compliance expertise, custom service delivery and strong commitment to solving security challenges and business issues. [www.solutionary.com](http://www.solutionary.com).