

## “SMALL BUSINESSES ARE NOW THE LOW HANGING FRUIT FOR CYBERCRIMINALS.”

FCC Chairman Julius Genachowski, October, 2011

### ARE YOU A TARGET?

According to security analyst's and fraud investigators contributing to a CNET report, "The Internet has bred an elite class of criminals who are organized, well funded and far more technologically sophisticated than law enforcement officials." Clearly, it is more important than ever to be proactive about network security, because once an intrusion happens, the damage has been done.

MJM can help you keep intruders out of your network, and keep you from becoming another statistic.

Contact us today to schedule a risk assessment for your business.

651.456.9307  
info@mjmitsolutions.com

Network Protection  
Layered Security

www.mjmitsolutions.com

technology  
consulting

- A 2010 survey of small and medium sized companies by Symantec Corp. reported that about 73% of businesses in the study had been targets of cyber attacks in the last year.
- In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at companies with 100 employees or fewer.
- According to the FBI, a handful of Trojans (a type of malicious software) engineered to steal on-line banking credentials were responsible for over \$100 million in losses to small businesses in the U.S. between mid-2009 and mid-2010.

### HOW SECURE IS YOUR NETWORK?

New technology and changing business strategies can boost your organization's productivity and sharpen your competitive edge. Yet at the same time, they can expose you to more security threats from both inside and outside your organization.

How do you evaluate those threats? An MJM Infrastructure Security Assessment will identify security vulnerabilities in your systems and make recommendations for practical, time-tested and cost effective security solutions.

Our security specialists are available should you need help applying any of the recommendations. Technology experts in multi-vendor environments, our qualified professionals can integrate these solutions into any network infrastructure.



An accurate assessment of your vulnerability to threats is crucial to minimizing the risk of business disruptions. An Infrastructure Security Assessment will enable your organization to:

- Identify vulnerabilities in systems protecting sensitive information assets.
- Identify a roadmap for eliminating or mitigating these vulnerabilities.
- Eliminate potential network security concerns of your customers and business partners.

### SIMPLIFYING YOUR SECURITY.

MJM IT Solutions offers technology thought leadership in tandem with our integration and support services. We deliver solutions that bridge the gap between your business and your IT infrastructure. Our innovative and proven counsel establishes a successful roadmap for the strategic planning, design, implementation & management of your IT infrastructure.

# FRAUD ADVISORY FOR BUSINESSES: CORPORATE ACCOUNT TAKEOVER

FBI Alert Issued 10-20-2010

## PROTECT:

- Educate everyone on this type of fraud scheme.
- Enhance the security of your PC's & network.
- Enhance the security of your corporate banking processes & protocols.
- Understand your responsibilities & liabilities.

## DETECT:

- Monitor & reconcile accounts at least once a day.
- Discuss options offered by your bank to help detect or prevent out-of-pattern activity.
- Note changes in the performance of your computer.
- Be on alert for rogue emails.
- Run regular virus & malware scans.

## RESPOND:

- If you detect suspicious activity, cease all online activity & remove all PC's that may be compromised from the network.
- Make sure employees know how & to whom to report suspicious activity to within your company and at your financial institution.
- Maintain a written chronology of what happened, what was lost and the steps taken to report the incident.

651.456.9307  
info@mjmitsolutions.com

www.mjmitsolutions.com

technology  
consulting

Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered.

To obtain access to financial accounts, cyber criminals target employees – often senior executives or accounting and HR personnel and business partners and cause the targeted individual to spread malicious software (or "malware") which in turn steals their personal information and log-in credentials. Once the account is compromised, the cyber criminal is able to electronically steal money from business accounts. Cyber criminals also use various attack methods to exploit check archiving and verification services that enable them to issue counterfeit checks, impersonate the customer over the phone to arrange funds transfers, mimic legitimate communication from the financial institution to verify transactions, create unauthorized wire transfers and ACH payments, or initiate other changes to the account. In addition to targeting account information, cyber criminals also seek to gain customer lists and/or proprietary information - often through the spread of malware - that can also cause indirect losses and reputational damage to a business.

First identified in 2006, this fraud, known as "corporate account take over," has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, **they have now begun to target municipalities, smaller businesses, and non-profit organizations.** Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Educating all stakeholders (financial institutions, businesses and consumers) on how to identify and protect themselves against this activity is the first step to combating cyber criminal activity.

## THINK YOUR MONEY'S SAFE?

*Consumers who bank online in the U.S. are protected by Federal Reserve Regulation E, which generally holds that consumers are not liable for unauthorized transactions against their bank accounts.*

*This provision does not apply to business account holders. If a company gets hacked and someone manages to clean out the firm's bank account, the company's bank is under no obligation to make that customer whole.*

## DO YOU HAVE A FALSE SENSE OF CYBER SECURITY?

According to a 2011 survey of U.S. small businesses, sponsored by Symantec and the National Cyber Security Alliance and conducted by Zogby International:

- 85% of small business owners said their company is safe from hackers, viruses, malware or a cyber-security breach.
- 77% said they do not have a written Internet security policy for employees.
- 59% do not use multifactor authentication (more than just a password) to access any of their networks.
- Only 8% are concerned about loss of customer information, 4% about loss of intellectual property and only 1% worry about loss of employee data, even though cyber security experts believe the loss of any of this kind of Information would be devastating to a business.

**Symantec.cloud**, through their heuristic based malware detection system, is currently detecting approximately 500,000 non-targeted, malware containing emails per day. 40.0% of all *targeted* attacks are being sent to SMB companies.

